

CLAIMS

1. A method of providing secure communication with kernel-level components of a computer system having an operating system that includes user space and kernel space, said method comprising the steps of:
 - (a) disposing an authentication module in the kernel space, in communicably coupled relation with the kernel-level components, to selectively encrypt and decrypt communications between the kernel-level components and a remote site;
 - (b) disposing a transport module in the kernel space, in communicably coupled relation with the authentication module, to selectively transmit and receive the communications; and
 - (c) selectively actuating the authentication module and the transport module to convey the communications to and from the kernel-level components.
2. The method of claim 1, comprising the step of communicably coupling the remote site to the kernel-level device by a network, and conveying the communications between the remote site and the kernel-level components while maintaining the communications free from the user space.
3. The method of claim 1, wherein the remote site is disposed within the user space of the computer system, and the communications pass from user space to the kernel-level components while encrypted.
4. The method of claim 1, further comprising the step of (d) disposing a filter driver in the kernel space in communicably coupled relation with the kernel-level components to intercept and selectively permit and prevent the communications from flowing to and from the kernel-level components.

5. The method of claim 4, comprising the steps of sequentially receiving communications from the remote site with the transport module, decrypting the communications with the authentication module, and alternatively permitting and preventing the communications from reaching the kernel-level components with the filter driver.
6. The method of claim 4, comprising the steps of sequentially actuating the filter driver to permit communications to pass from the kernel-level components, encrypting the communications with the authentication module, and transmitting the communications with the transport module.
7. The method of claim 4, further comprising the step of (e) providing a management module to selectively actuate the filter driver, the authentication module, and the transport module to convey the communications to and from the kernel-level components.
8. The method of claim 7, comprising the step of disposing the management module in the kernel space.
9. The method of claim 1, wherein the transport module comprises a kernel sockets module and a communication server, the kernel sockets module and the communication server being disposed within the kernel space.
10. The method of claim 4, further comprising the steps of:
 - (f) providing a service context module to define a plurality of operational states in which the computer may perform a plurality of operations; and
 - (g) configuring the filter driver to selectively permit and prevent the performance of the operations by permitting and preventing communications pertaining to the operations when the computer system is disposed in each of the operational states, wherein at least one of the plurality of operations is permitted when the computer system is disposed in a

first one of the operational states and prevented when the computer system is disposed in a second one of the operational states.

11. The method of claim 10, wherein the plurality of states comprise an operational state and an administrative state.
12. The method of claim 10, further comprising the step of using a user interface to selectively place the computer system into one of the states.
13. The method of claim 12, wherein the user interface effects the using a user interface step, using encrypted communication with a service context manager disposed in the kernel space.
14. A method of providing secure communication with kernel-level components of a computer system having an operating system that includes user space and kernel space, said method comprising the steps of:
 - (a) disposing a filter driver in the kernel space to selectively permit and prevent communications with the kernel-level components;
 - (b) disposing an authentication module in the kernel space, in communicably coupled relation with the filter driver, to selectively encrypt and decrypt the communications; and
 - (c) disposing a transport module in the kernel space, in communicably coupled relation with the authentication module, to selectively transmit and receive the communications;
 - (d) actuating the filter driver, authentication module, and transport module to respectively convey received and transmitted communications to and from the kernel-level components.
15. A system for providing secure communication between a remote site and kernel-level components of a computer having user space and kernel space, the system comprising:

a filter driver disposed in the kernel space to selectively permit and prevent communications with the kernel-level components;

an authentication module disposed in the kernel space, in communicably coupled relation with the filter driver, to selectively encrypt and decrypt the communications;

a transport module disposed in the kernel space, in communicably coupled relation with the authentication module, to selectively transmit and receive the communications; and

a remote authentication module disposed in the remote site, in communicably coupled relation with the transport module, to selectively decrypt and encrypt the communications in cooperation with the authentication module;

wherein communications from the remote site to the kernel-level components are sequentially encrypted by the remote authentication module, received by the transport module, decrypted by the authentication module, and selectively permitted to reach the kernel-level components by the filter driver, and communications generated by the kernel-level components are sequentially permitted by the filter driver, encrypted by the authentication module, transmitted by the transport module, and decrypted by the remote authentication module.

16. The system of claim 15, wherein the remote site is discrete from the computer and the communications are conveyed between the remote site and the kernel-level components while being free from the user space.
17. The system of claim 15, wherein the remote site is disposed within the user space of the computer and the communications are conveyed between the user space and the kernel-level components while encrypted.

18. An article of manufacture for providing secure communications with kernel-level components of a computer system having an operating system that includes user space and kernel space, said article of manufacture comprising:

a computer usable medium having computer readable program code embodied therein, said computer usable medium having:

computer readable program code for defining an authentication module in the kernel space, in communicably coupled relation with the kernel-level components, to selectively encrypt and decrypt communications between the kernel-level components and a remote site;

computer readable program code for defining a transport module in the kernel space, in communicably coupled relation with the authentication module, to selectively transmit and receive the communications; and

computer readable program code for selectively actuating the authentication module and the transport module to convey the communications to and from the kernel-level components.

19. Computer readable program code for providing secure communications with kernel-level components of a computer system having an operating system that includes user space and kernel space, said computer readable program code comprising:

computer readable program code for defining an authentication module in the kernel space, in communicably coupled relation with the kernel-level components, to selectively encrypt and decrypt communications between the kernel-level components and a remote site;

computer readable program code for defining a transport module in the kernel space, in communicably coupled relation with the authentication module, to selectively transmit and receive the communications; and

computer readable program code for selectively actuating the authentication module and the transport module to convey the communications to and from the kernel-level components.

20. The computer readable program code of claim 19, comprising computer readable program code for intercepting communications from the remote site to destinations within kernel space and selectively permitting and preventing the communications from reaching the destinations.
21. The computer readable program code of claim 20, comprising one or more shims disposed within the kernel space to intercept the communications.
22. The computer readable program code of claim method of claim 19, comprising computer readable program code for using encrypted communications to selectively place the computer system into one of said states.